

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Samsung cellular telephone, Serial # R58JA5M7X6E

Case No.

18-746-m

FILED

MAY 10 2018

APPLICATION FOR A SEARCH WARRANT

KATE DARIKMAN, Clerk
By _____ Dep. Clerk

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Samsung cellular telephone, Serial # R58JA5M7X6E

located in the _____ Eastern _____ District of _____ Pennsylvania _____, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, United States Code,
Sections 1029(a)(4) and
1028A

Offense Description

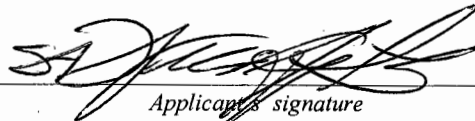
Access device fraud conspiracy and aggravated identity theft

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

William Aquilani

Printed name and title

Sworn to before me and signed in my presence.

Date:

May 10, 2018

City and state: Philadelphia, PA



Judge's signature

Lynne A. Sitarshi, U.S. Magistrate Judge

Printed name and title

18-746-m

FILED

MAY 10 2018

**AFFIDAVIT OF SPECIAL AGENT WILLIAM AQUILANI
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

KATE BARKMAN, Clerk
By: _____ Dep. Clerk

I, WILLIAM AQUILANI, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent employed by Homeland Security Investigations (“HSI”), an agency within the U.S. Department of Homeland Security (“DHS”), Immigration and Customs Enforcement (“ICE”). I am currently assigned to Cyber Crimes Investigations Group within the HSI office in Philadelphia, Pennsylvania. I have been employed by HSI and its legacy component agencies as a Special Agent since August 1997. I have a Bachelor of Arts degree in Political Science and am a graduate of the Federal Law Enforcement Training Center in Brunswick, Georgia. I have conducted and participated in numerous investigations including but not limited to financial crimes, narcotics violations, immigration offenses, and other violations of Title 18 of the United States Code.

2. I am an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516. As such, I am an “investigative or law enforcement officer” within the meaning of 18 U.S.C. § 2510(7).

3. The information in this affidavit is based on personal knowledge as well as conversations with other law enforcement officers and agents and my review of various records, including investigative reports, photographs and surveillance video. Because I submit this affidavit for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish a foundation for the issuance of a warrant.

II. PURPOSE OF WARRANT

4. I submit this Affidavit for the limited purpose of obtaining a federal search warrant for the following cellular telephone/mobile device (hereinafter referred to as the SUBJECT DEVICE):

Samsung cellular phone, serial number #R58JA5M7X6E

5. As explained below, I submit that probable causes exist to believe that the SUBJECT DEVICE contains evidence of the offenses of conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029(a)(4), (b)(2); access device fraud, in violation of 18 U.S.C. § 1029(a)(4); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1).

III. PROBABLE CAUSE AND FACTUAL BACKGROUND

6. GEORGE IACOB is a citizen and national of Romania. He was born on April 23, 1985 in Romania. IACOB entered the United States illegally at or near Rio Grande Valley, Texas, on August 28, 2017, and was apprehended by the United States Border Patrol. IACOB was put into deportation proceedings for illegally entering the United States. IACOB made claims for credible fear if returned to Romania and was subsequently released on an immigration bond with Immigration and Customs Enforcement (ICE) pending his asylum and removal hearings. IACOB is currently still in removal proceedings. An ICE detainer was lodged on IACOB at the Federal Detention Center in Philadelphia, Pennsylvania.

IV. PENNSYLVANIA STATE POLICE INVESTIGATION

CFCU – CONCORD BRANCH ATM COMPROMISE

7. On November 3, 2017, R.M., the Assistant Manager of the Citadel Federal Credit Union's (CFCU) Concord Branch, located at 901 Baltimore Pike, Concord Township, PA,

conducted his routine inspection of the branch's drive-up ATM for tampering and serviceability prior to opening the branch to customers. During this inspection, he discovered an anomaly with the ATM near the card swipe mechanism. He then disabled the ATM from customer usage and notified the bank's security department. No further use of the ATM occurred until a CFCU technician discovered the presence of an unauthorized device, consistent with a skimmer, affixed to the card swipe mechanism of the ATM.

8. R.M. learned from the security department of the presence of a blue minivan, bearing New Jersey registration number U27GEP, that was captured via surveillance video on November 2, and November 3, 2017, and that the male driver of the vehicle attempted to shield his face from the security cameras during his encounters at the ATM. R.M. had physically observed this minivan at approximately 1230 and 1300 hours on November 3, 2017 at the bank's ATM. The vehicle's operator drew R.M.'s attention because the operator was shielding his face while manipulating the face of the ATM with an outstretched arm in an up and down motion on both occasions. R.M. provided a description of the male driver of the vehicle and the vehicle to the Pennsylvania State Police.

9. On November 3, 2017, at approximately 1236 hours, R.M. contacted the Pennsylvania State Police (PSP) regarding the discovery of tampering of the bank's drive-up ATM and the unauthorized device that had been affixed to the card swipe mechanism of the ATM, along with the information regarding the suspect's vehicle. At approximately 1315 hours, the aforementioned vehicle was located by the PSP, who confirmed that the vehicle, a blue Chrysler Town & Country minivan, was under active suspension from the state of New Jersey. A traffic stop of the vehicle led to the identification of the driver as Alexandru VELCU via Romanian identification cards that he produced. VELCU did not have a valid driver's license

issued in the United States. Due to the non-United States identification documents, VELCU was transported to the PSP Media Barracks for positive identification via LiveScan fingerprinting.

10. Meanwhile, PSP Trooper Gibson went to CFCU and was provided with the ATM card swipe device which was retrieved from the ATM and external surveillance video for November 2, and November 3, 2017. The surveillance video revealed the following instances:

a. On November 2, 2017, at approximately 2147 hours, a blue minivan appeared at the ATM machine. The driver's side sliding door opened and revealed two masked individuals sitting in the second row. The driver, wearing a blue hooded sweatshirt bearing a large Nike brand logo on the back, was subsequently identified as VELCU. One of the passengers, believed to be a white male, was dressed all in black, including a black baseball cap bearing the words, "Cata Boss," and a half ski mask. For approximately three minutes, this second individual was captured on the video while he retrieved items handed to him by VELCU, then repetitively stroking his arm back and forth with a bank-type card toward the face of the ATM.

b. On November 3, 2017, at approximately 0626 hours, the same blue minivan returned to the drive-up ATM. Through the driver's window glass, an individual, later identified as VELCU, can be observed wearing a black long-sleeve shirt bearing a white-patterned design on the shoulder area, black baseball cap with grey brim, and a large wrist watch on the left wrist. When the driver's side sliding door opened, a heavy-set male, wearing a half ski mask and blue hooded Nike branded sweatshirt with red trim along the waist and sleeve wrist area, emerged. For approximately five minutes, the latter individual retrieved items from the minivan, and used super glue and a long slender metal object on the face of the ATM to manipulate the machine.

c. On November 3, 2017, at approximately 1255 hours, the same minivan reappeared at the drive-up ATM. The driver, later identified as VELCU, was visible wearing a blue Nike sweatshirt with red trim and a baseball cap with a grey brim. With his right hand, VELCU attempted to shield his face with a dark cloth or object. With his left hand, he inserted a card-like object into the ATM, while moving his head from side-to-side. After approximately one minute, VELCU seemed to speed away from the ATM. At approximately 1306 hours, VELCU drove up to the ATM in the same vehicle and used his left hand to insert a card-like object into the face of the ATM. After approximately one minute, VELCU departed the machine.

11. An analysis of the device recovered from within the interior portion of the card slot of CFCU's drive-up ATM was conducted. The device can best be described as a foreign electronic device comprised generically of a computer chip and metal arm bearing electronic contacts positioned in manner where said contacts would be positioned over the magnetic stripe area of a bank card having been placed within the card reader when installed in an ATM. CFCU's technician will testify that the device is intended to capture account numbers.

12. According to CFCU's Risk Management Senior Analyst, at no time did the occupants of the minivan perform a legitimate ATM transaction. However, four persons with ATM/Bank cards and their accounts were compromised between the time VELCU was first present at the ATM and when the ATM was disabled, including the patron whose account number was found on the gift card in VELCU's possession at the time of his arrest.

CFCU – SPRINGFIELD BRANCH ATM COMPROMISE

13. CFCU's Risk Management Senior Analyst obtained surveillance video from the bank's Springfield Branch, which shows:

a. The same minivan that was captured on surveillance video at the Concord Branch on November 2, and November 3, 2017, was captured on surveillance video at the Springfield Branch beginning on November 1, 2017, at approximately 0615 hours, at the branch's drive-up ATM. The camera also captured images of the driver, a front seat passenger, and a rear seat passenger. When the driver's side sliding door opened, the rear seated passenger's image was made clearer and revealed a white male who attempted to shield his face. He wore a black, "bubble-type" coat and blue vest. During actions captured for five minutes, this individual retrieved items from the minivan, used super glue on an object, and presented a long, slender object that appears to have electronic circuitry, all of which were used to manipulate the ATM. His actions bear a striking resemblance to that which was observed at the Concord Branch and the items used are consistent with those seized from VELCU's vehicle pursuant to a vehicle search warrant.

b. On November 1, 2017, at approximately 1155 hours, the same blue minivan being driven by an individual who matched VELCU's facial image, appeared on surveillance video at the drive-up ATM. Over the course of 52 seconds, the driver's side passenger sliding door opened and an unmasked white male wearing distinct eyeglasses and a black, "bubble-type" coat, emerged. This individual projected a card-type object toward the ATM, and retracted it. Once the individual retracted the object, he and the minivan departed. HSI Special Agent John Hedrick identified the passenger in this video to George IACOB based upon an arrest photograph of IACOB contained in an Immigration and Customs Enforcement database.

c. At approximately 1925 hours, the same minivan reappeared at the drive-up ATM. The driver's window of the vehicle opened and the male driver attempted to cover his

face with a cloth-like object, but his image is consistent with that of VELCU, including the same wrist watch that was seized at the time of his arrest, referenced below. The appearance of the front seat passenger was also captured and matched that of IACOB. For approximately one minute, VELCU projected a card-type object toward the ATM's face and manipulated same.

d. On November 2, 2017, at approximately 1836 hours, the same blue minivan that appeared on November 1, 2017, reappeared at the drive-up ATM. When the driver's side sliding passenger door opened, a man wearing a half ski mask and black ball cap bearing the words "Cata Boss" is seen in the second row passenger area and is believed to be IACOB. Said male is of the same complexion, build and mannerism as the man also believed to be IACOB depicted in the November 1, 2017, at 1155 hours, video who was unmasked at the time. The vehicle's driver wore a blue Nike-branded hooded sweatshirt. Over the course of the nearly one minute, the individual, believed to be IACOB, retrieved metallic/electronic items from the ATM and placed them inside the minivan. The driver of the minivan then departed in an expeditious manner.

14. According to CFCU's Risk Management Senior Analyst, at no time did the occupants of the minivan perform a legitimate ATM transaction. However, 134 persons with ATM/Bank cards and their accounts were compromised between the time the occupants of the minivan was first present at the ATM and when the ATM was disabled because of the revelation of the skimming device.

VELCU'S ARREST AND SEARCH OF MINIVAN AND PHONE

15. When VELCU was stopped by the PSP and taken into custody on November 3, 2017, he was wearing a blue Nike sweatshirt with a large Nike logo on the back, consistent with the one captured on surveillance video at 2147 hours on November 2, 2017. He was also

wearing a black baseball cap with a grey brim, a black long-sleeve shirt bearing a white-patterned design on the shoulder area, black baseball cap with grey brim, and a large wrist watch on the left wrist consistent with the same items captured on surveillance video at 0626 hours on November 3, 2017. VELCU was also in possession of a gift card with a Visa brand; it was later determined that the account number embossed on the card did not match the account number contained on the card's magnetic strip and that the account number was in VELCU's possession without the owner of the account number's authorization.

16. VELCU was afforded his Miranda Rights, which he waived and signed a waiver form. Afterwards, VECLU stated that he receives instructions from unidentified Mexicans to go to banks in order to "insert cards and push buttons." He said he is paid \$200-\$300 for performing this action, but failed to convey the ultimate objective intended. When shown surveillance photographs captured via CFCU's surveillance cameras, specifically from the segment of video from November 2, 107 at 2147 hours, VELCU denied knowing the male passenger and denied that he was the driver of the minivan, despite being dressed in the exact same manner as the driver.

17. Subsequent to VELCU's arrest, a state search warrant was executed upon his minivan. The following items were seized:

- black baseball cap, bearing the words "Cata Boss"
- Motorola Droid cellular telephone
- Neoprene ski mask
- Pair of knit gloves
- Starbuck gift card, bearing sandpaper

Noted during the search, but not seized, was a bottle of super glue within the 2nd row passenger area floorboard.

18. A warrant was also obtained to search VELCU's phones. On November 24, 2017, PSP Trooper Gibson received the forensic analysis of results of VELCU's mobile phones. The points of interest are as follows:

a. Contained on the iPhone was a text message thread from November 3, 2017, to a New York phone number ending with 7130. Text and picture messages were exchanged soliciting fraudulent identification credentials, namely a driver's license, for IACOB, in exchange for money. A photograph with name "George IACOB" and date of birth "04/23/85" was also transmitted, seemingly the subject of the sought-after credentials.

b. Two screen-captures from the US Department of Homeland Security's official webpage, namely the "detainee locator" tool-depicting search results for a "George Iacob" with associated Alien number "213133027."

c. Two screen-capture type images of two separate CFCU locations (Warminster and Phoenixville, PA). The Warminster Branch specifically states "ATM (Citadel)."

V. THE SUBJECT DEVICE

19. On March 15, 2018, a federal grand jury returned an indictment charging IACOB with conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029(a)(4), (b)(2) (Count One); access device fraud, in violation of 18 U.S.C. § 1029(a)(4) (Count Two).

20. On April 25, 2018, IACOB made his initial appearance in the Eastern District of Pennsylvania on the indictment.

21. IACOB's cell phone, the SUBJECT DEVICE, and other personal effects of IACOB were mailed to your Affiant from Minnesota, where IACOB was previously in the custody of the Hennepin County Prison in Minnesota on an unrelated charge. The SUBJECT DEVICE is a Samsung cellular phone bearing serial number #R58JA5M7X6E

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Cellular telephone: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the telephone. In addition to enabling voice communications, cellular telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and telephone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a device that records still and moving images digitally. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media

include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store any digital data, such as word processing documents, even if the device is not designed to access such files. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, I know that electronic devices, such as the SUBJECT DEVICE, have capabilities that allow them to serve as a cellular telephone, digital camera, portable media player, and PDA.

VII. ELECTRONIC DEVICES AND STORAGE

24. As described above and in Attachment A, this application seeks permission to search and seize things that the SUBJECT DEVICE may contain, in whatever form they are stored. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information from a device,

it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. Searching for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment A, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, HSI intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

26. Based upon my experience and training, as well as my discussions with other law enforcement officers, I have learned that owners of cellular phones have the option of creating a password that must be used to gain entry into either the entire database or a particular option therein. If the law enforcement officers who execute this search warrant cannot gain access to all of the databases within the cellular telephones, then permission is respectfully requested to permit the officers to obtain the assistance of representatives of the manufacturer of the cellular telephones or another expert in overriding the security mechanisms and gaining entry to all of the

databases within the cellular telephones so that law enforcement may examine the contents of the cellular telephones.

VIII. CONCLUSION

27. I believe from my training and experience and from review of the specifications for cellular telephones by others participating in this investigation, that such devices are capable of routinely storing data, including but not limited to: telephone directory entries consisting of names, addresses and telephone numbers; logs of telephone numbers dialed; telephone numbers of missed calls; telephone numbers of received calls; schedule entries; emails; text messages; website addresses; visited websites; stored memoranda, emails and text documents; and stored voicemail message and stored digital photographs.

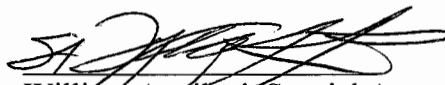
28. I believe probable cause exists to permit a search of the memory and information stored within the cellular telephone listed above will yield evidence of violations of the federal fraud laws, including, but not limited to, evidence disclosing the identities of persons involved in the commission of various fraud related offenses. It is also likely that photographs stored in the devices will reveal the identities of others involved in the financial fraud offenses and the locations where they operate.

29. I believe that there is probable cause to believe the SUBJECT DEVICE was used to facilitate access device fraud, bank fraud and aggravated identity theft, and that a search of the memory and data stored on these telephones will yield additional evidence of violations of these federal fraud laws, as well as, other evidence disclosing the identities of persons involved in the commission of these offenses. It is also expected that this search will disclose evidence of calls made by and to others involved in the course of the events related in this affidavit.

30. Based on the above, I submit that there is probable cause to believe that GEORGE IACOB, and others, together conspired to obtain, and succeeded in obtaining, stolen and altered credit and/or debit card account numbers by utilizing an ATM skimming device or access device, to obtain real persons' account numbers, and conspired and attempted to commit access device fraud, in violation of 18 U.S.C. § 1029(a)(4), (b)(2); access device fraud, in violation of 18 U.S.C. § 1029(a)(4); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1).

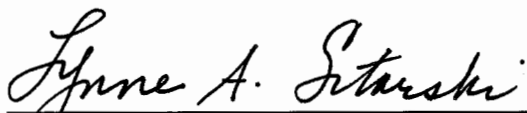
31. For all of the foregoing reasons, your affiant respectfully requests that the Court approve a search warrant for the SUBJECT DEVICE. I affirm under penalty of perjury that the above information is true and correct to the best of my knowledge.

Respectfully submitted



William Aquilani, Special Agent
Homeland Security Investigations
U.S. Department of Homeland Security

Sworn to and subscribed before me this 10th day of May 2018.



HONORABLE LYNNE A. SITARSKI
United States Magistrate Judge